31 JAN 1980

MEMORANDUM FOR: Mr. Douglas Cannon
Deputy Team Leader, Logistics & Communications
Division/GAO

STATINTL FROM : [redacted]
Chief, Information Services Staff

SUBJECT : CIA's Implementation of the Systematic Review Requirements of E.O. 12065 and its Predecessor E.O. 11652

STATINTL REFERENCE : Telephone Conversations of 4 and 7 January 1980 [redacted] Concerning Specific GAO Questions

1. Your questions and answers thereto are set forth below in logical sequence:

Q. Status of Records Schedules - total holdings with percent permanent and temporary.

A. The Agency has Records Control Schedules approved by the National Archives and Records Service identifying permanent and temporary records. However, a precise percentage breakdown of permanent and temporary records depends upon: (1) completion of our records review which under ISOO Directive No. 1 isn't due until December 1, 1980; and (b) updating of our records control schedules. At this point the estimated Agency total records holdings, both permanent and temporary, is 274,997 cubic feet of record. 224,199 cubic feet are considered temporary - an estimated 50,798 cubic feet are permanent as follows:

		TOTAL (cu. ft.)	PERMANENT (cu. ft.)
ARCHIVES		24,497	24,497
RECORDS CENTER		68,517	10,812
HEADQUARTERS		181,983	
Constituting:			
DCI	5,237	estimative factor of	
DDA	48,935	x 5% = 2,708	
DDO	32,416		15,489
DDS&T	40,441	estimative factor of	
NFAC	54,954	x 10% = 12,781	
		ESTIMATED TOTAL PERMANENT RECORDS	50,798

Q. Estimate of percent of CIA records which must be reviewed document by document as opposed to bulk declassification.

A. Generally all CIA permanent records must be reviewed document by document to avoid the inadvertent declassification of national security information meeting the classification criteria of E.O. 12065. Certain unique files, such as chrono files of an office, which are largely classified and in which file integrity is essential, may be reviewed on a folder basis. Under this procedure, the file is reviewed as a single document. Classification of the file is maintained with each document stamped for individual review if it is requested under the FOIA or Mandatory review provisions of E.O. 12065.

Q. Number of pages reviewed to date and percent declassified - OSS vs. CIG/CIA.

A. CIA has reviewed 862 cubic feet or 1,724,000 pages of OSS permanent records for accessioning to NARS, of which a first increment of 200 cubic feet has been accessioned. Over 90% of OSS material reviewed thus far has been declassified. CIA has systematically reviewed 1,166,384 pages of CIG/CIA information 20 years of age or older of which 58,161 pages or 4.98% has been declassified. Declassification of later information varies according to category. For example, of 855 documents constituting 9,786 pages of older (1947-1950) finished intelligence reports reviewed, 7,133 pages or 72.9% were declassified. On the other hand no permanent information on certain sensitive operations can be declassified.

Q. The estimated number of pages of permanent records to be reviewed by 1988. Rate of review with current and projected resources. Shortfall if any.

A. Of the estimated 50,798 cubic feet of permanent records, some 25% are "guesstimated" as 20 years of age or older. An additional 25% are estimated as becoming 20 years of age or older by 1988. The estimated workload to be accomplished by 1 December 1988 is therefore half of the permanent records or 25,399 cubic feet. At 2,000 pages per cubic foot, the estimated number of pages to be reviewed by 1988 is 50,798,000. In FY 79, excluding OSS documents, 20 CIA review officers systematically reviewed over a period of 250 work days, nearly 700,000 pages of material. An additional 11 personnel were involved as intelligence assistants, data inputers, secretaries, and managers. The rate of review was 140 pages per day per reviewer. Estimated number of pages reviewed per year at the FY 79 rate are: FY 80 - 1,050,000; FY 81-84 - 1,225,000; and FY 85-88 - 1,330,000; or a total of 11,270,000 pages. This number amounts to 22% of the estimated workload to be completed during the period FY 80 through 1988 leaving a shortfall of 78%.

Q. The number of CIA personnel working on systematic review for declassification and the yearly cost beginning with FY 73 to FY 80 with projections for FY 81 - FY 88.

A. CIA personnel allocated to systematic review and costs incurred are set forth below beginning with FY 73 and continuing through FY 88. It should be noted that CIA's review program began modestly in FY 73 with 3 part-time independent contractors to review OSS documents. This part of the systematic review program subsequently increased to 15 part-time independent contractors at an annual cost of $160,000. This allocation rate of personnel and funds for OSS documents is projected through FY 83 when hopefully all OSS documents will have been systematically reviewed.

In FY 77 and FY 78 components began to detail personnel for the systematic review program pending the authorization of required new positions. In FY 79, 39 new positions were authorized for the systematic review program with an additional 5 positions projected for FY 81. Approval was also secured to hire retired annuitants as part-time contract employees equivalent to 8 AE. A 5% inflation factor is included in cost projections beginning in FY 82.

FISCAL YEAR	NO. OF PERSONNEL	COSTS
1973	3	$ 31,500
1974	7	65,000
1975	10	94,484
1976	15	143,650
1977	25	421,820
1978	30	547,022
1979	46	1,038,277
1980	57	1,647,000
1981	62	1,728,000
1982	62	1,806,400
1983	62	1,896,720
1984	47	1,823,556
1985	50	2,019,600
1986	50	2,120,580
1987	50	2,226,609
1988	50	2,337,939
	TOTAL	$19,948,157

Q. If CIA were relieved of the systematic review requirement and continued mandatory review only, what would be the saving.

A. Excluding OSS permanent records for which we believe systematic review should be completed at modest cost by the end of FY 83, it will cost beginning in FY 80 an estimated $17,606,404 to accomplish 22% of CIA's estimated workload to be completed by 1988. The savings would be tremendous if CIA were relieved of the systematic review requirement and serviced only mandatory review requests. In 1978 CIA spent $260,000 servicing mandatory review requests and a comparable amount in 1979. If $260,000 for mandatory review requests is projected for the years FY 80 - FY 88 the cost is $2,340,000. This amount compares to an estimated $17,606,404 for systematic review for the same period to accomplish only 22% of the task. Estimated savings would be $15,266,404. It should also be recognized that overall most intelligence permanent records cannot be declassified for reasons of national security. Relief from the systematic review requirement of E.O. 12065 would not only enable funds and personnel to be directed against high priority intelligence objectives, but would also lesson the possibility of error in releasing sensitive information which could result in serious damage to national security. The latter possibility increases in a worsening international environment when release of older information about a country whose government has changed could adversely affect U.S. relations with the new government. Finally, it could be noted that if personnel were allocated to complete by 1988 the estimated workload of permanent records, the cost would be in the neighborhood of $80,000,000.

2. Guidelines as listed below governing the systematic review program are attached:

a. Guidelines for Classification Review of CIA Predecessor Records and Information Between 1941-1946;

b. Review of Foreign Government Information (OSS Documents);

c. Guidelines for the Review of Records for the Period From the End of OSS to the Beginning of CIA 1 October 1945 - 20 September 1947;

d. CIA Systematic Review Guidelines;

e. Guidelines for Systematic Review of Foreign Government Information Thirty Years Old or Older;

f. Special Procedures for Use in Systematic Review of Cryptologic Information Pursuant to Section 3-403 of Executive Order 12065; and

g. Categories of Information for Which the Director of the Information Security Oversight Office (ISOO) Has Granted Waivers of the 10-year Review Requirement of Section 3-401 of Executive Order 12065.

3. It is requested that information provided by CIA and included in proposed GAO reports be checked with CIA from the standpoints of classification and use prior to publication.

[redacted] STATINTL

Attachments: a/s

Next 1 Page(s) In Document Exempt

Approved For Release 2002/02/14 : CIA-RDP85B00236R000100170009-7

CENTRAL INTELLIGENCE AGENCY

WASHINGTON, D.C. 20505

5 February 1980

MEMORANDUM FOR: Mr. Douglas Cannon
Deputy Team Leader
Logistics & Communications Division, GAO

STATINTL FROM: [redacted]
Chief, Information Services Staff
Directorate of Administration

SUBJECT: CIA's Implementation of the Systematic Review Requirements of E.O. 12065 and its Predecessor E.O. 11652

REFERENCE: Telephone Conversations of 4 and 7 January 1980 Between
STATINTL [redacted] Concerning Specific GAO Questions

1. Your questions and answers thereto are set forth below in logical sequence:

Q. Status of Records Schedules - total holdings with percent permanent and temporary.

A. The Agency has Records Control Schedules approved by the National Archives and Records Service identifying permanent and temporary records. However, a precise percentage breakdown of permanent and temporary records depends upon: (1) completion of our records review which under ISOO Directive No. 1 isn't due until December 1, 1980; and (2) updating of our records control schedules. At this point the estimated Agency total records holdings, both permanent and temporary, is 274,997 cubic feet of records. 224,199 cubic feet are considered temporary -- an estimated 50,798 cubic feet are permanent as follows:

	TOTAL (cu. ft.)	PERMANENT (cu. ft.)
ARCHIVES	24,497	24,497
RECORDS CENTER	68,517	10,812
HEADQUARTERS	181,983	
Constituting:		
DCI 5,237	estimative factor of	
DDA 48,935	x 5% = 2,708	
DDO 32,416		15,489
DDS&T 40,441	estimative factor of	
NFAC 54,954	x 10% = 12,781	
ESTIMATED TOTAL PERMANENT RECORDS		50,798

Q. Estimate of percent of CIA records which must be reviewed document by document as opposed to bulk declassification.

A. Generally all CIA permanent records must be reviewed document by document to avoid the inadvertent declassification of national security information meeting the classification criteria of E.O. 12065. Certain unique files, such as chrono files of an office, which are largely classified and in which file integrity is essential, may be reviewed on a folder basis. Under this procedure, the file is reviewed as a single document. Classification of the file is maintained with each document stamped for individual review if it is requested under the FOIA or Mandatory review provisions of E.O. 12065.

Q. Number of pages reviewed to date and percent declassified - OSS vs. CIG/CIA.

A. CIA has reviewed 862 cubic feet or 1,724,000 pages of OSS permanent records for accessioning to NARS, of which a first increment of 200 cubic feet has been accessioned. Over 90% of OSS material reviewed thus far has been declassified. CIA has systematically reviewed 1,166,384 pages of CIG/CIA information 20 years of age or older of which 58,161 pages or 4.98% has been declassified. Declassification of later information varies according to category. For example, of 855 documents constituting 9,786 pages of older (1947-1950) finished intelligence reports reviewed, 7,133 pages or 72.9% were declassified. On the other hand no permanent information on certain sensitive operations can be declassified.

Q. The estimated number of pages of permanent records to be reviewed by 1988. Rate of review with current and projected resources. Shortfall if any.

A. Of the estimated 50,798 cubic feet of permanent records, some 25% are "guesstimated" as 20 years of age or older. An additional 25% are estimated as becoming 20 years of age or older by 1988. The estimated workload to be accomplished by 1 December 1988 is therefore half of the permanent records or 25,399 cubic feet. At 2,000 pages per cubic foot, the estimated number of pages to be reviewed by 1988 is 50,798,000. In FY 79, excluding OSS documents, 20 CIA review officers systematically reviewed over a period of 250 work days, nearly 700,000 pages of material. An additional 11 personnel were involved as intelligence assistants, data inputers, secretaries, and managers. The rate of review was 140 pages per day per reviewer. Estimated number of pages reviewed per year at the FY 79 rate are: FY 80 - 1,050,000; FY 81-84 - 1,225,000; and FY 85-88 - 1,330,000; or a total of 11,270,000 pages. This number amounts to 22% of the estimated workload to be completed during the period FY 80 through 1988 leaving a shortfall of 78%.

Q. The number of CIA personnel working on systematic review for declassification and the yearly cost beginning with FY 73 to FY 80 with projections for FY 81 - FY 88.

A. CIA personnel allocated to systematic review and costs incurred are set forth below beginning with FY 73 and continuing through FY 88. It should be noted that CIA's review program began modestly in FY 73 with 3 part-time independent contractors to review OSS documents. This part of the systematic review program subsequently increased to 15 part-time independent contractors at an annual cost of $160,000. This allocation rate of personnel and funds for OSS documents is projected through FY 83 when hopefully all OSS documents will have been systematically reviewed.

In FY 77 and FY 78 components began to detail personnel for the systematic review program pending the authorization of required new positions. In FY 79, 39 new positions were authorized for the systematic review program with an additional 5 positions projected for FY 81. Approval was also secured to hire retired annuitants as part-time contract employees equivalent to 8 AE. A 5% inflation factor is included in cost projections beginning in FY 82.

FISCAL YEAR	NO. OF PERSONNEL	COSTS
1973	3	$ 31,500
1974	7	65,000
1975	10	94,484
1976	15	143,650
1977	25	421,820
1978	30	547,022
1979	46	1,038,277
1980	57	1,647,000
1981	62	1,728,000
1982	62	1,806,400
1983	62	1,896,720
1984	47	1,823,556
1985	50	2,019,600
1986	50	2,120,580
1987	50	2,226,609
1988	50	2,337,939
	TOTAL	$19,948,157

Q. If CIA were relieved of the systematic review requirement and continued mandatory review only, what would be the saving.

A. Excluding OSS permanent records for which we believe systematic review should be completed at modest cost by the end of FY 83, it will cost beginning in FY 80 an estimated $17,606,404 to accomplish 22% of CIA's estimated workload to be completed by 1988. The savings would be tremendous if CIA were relieved of the systematic review requirement and serviced only mandatory review requests. In 1978 CIA spent $260,000 servicing mandatory review requests and a comparable amount in 1979. If $260,000 for mandatory review requests is projected for the years FY 80 - FY 88 the cost is $2,340,000. This amount compares to an estimated $17,606,404 for systematic review for the same period to accomplish only 22% of the task. Estimated savings would be $15,266,404. It should also be recognized that overall most intelligence permanent records cannot be declassified for reasons of national security. Relief from the systematic review requirement of E.O. 12065 would not only enable funds and personnel to be directed against high priority intelligence objectives, but would also lessen the possibility of error in releasing sensitive information which could result in serious damage to national security. The latter possibility increases in a worsening international environment when release of older information about a country whose government has changed could adversely affect U.S. relations with the new government. Finally, it could be noted that if personnel were allocated to complete by 1988 the estimated workload of permanent records, the cost would be in the neighborhood of $80,000,000.

2. Guidelines as listed below governing the systematic review program are attached:

a. Guidelines for Classification Review of CIA Predecessor Records and Information Between 1941-1946;

b. Review of Foreign Government Information (OSS Documents);

c. Guidelines for the Review of Records for the Period From the End of OSS to the Beginning of CIA 1 October 1945 - 20 September 1947;

d. CIA Systematic Review Guidelines;

e. Guidelines for Systematic Review of Foreign Government Information Thirty Years Old or Older;

f. Special Procedures for Use in Systematic Review of Cryptologic Information Pursuant to Section 3-403 of Executive Order 12065; and

g. Categories of Information for Which the Director of the Information Security Oversight Office (ISOO) Has Granted Waivers of the 10-year Review Requirement of Section 3-401 of Executive Order 12065.

3. It is requested that information provided by CIA and included in proposed GAO reports be checked with CIA from the standpoints of classification and use prior to publication. STATINTL

[redacted]

Attachments: a/s

11 December 1978

GUIDELINES FOR CLASSIFICATION REVIEW OF CIA PREDECESSOR RECORDS AND INFORMATION BETWEEN 1941-1946

These guidelines are for use in reviewing the classification of permanent records of the Coordinator of Information (COI), (in existence from July 1941 to June 1942); the Office of Strategic Services (OSS), (June 1942 to September 1945); and the Strategic Services Unit (SSU), (October 1945 to October 1946) for which the Director of the CIA has responsibility. Executive Order 12065 requires that classified information constituting permanently valuable records of the government, as defined by 44 U.S.C. 2103, shall be reviewed for declassification as it becomes twenty years old or thirty years in the case of foreign government information. The Order further requires that guidelines for systematic review for declassification shall be issued and state specific limited categories of information which, because of their national security sensitivity, should not be declassified automatically but should be reviewed item-by-item to determine whether continued protection is needed.

A document can only be exempted from declassification if information contained therein is exempt by statute from declassification or meets a two-step test:

1. It concerns one or more of the classification requirements set forth in Section 1-301 of Order:

   (a) military plans, weapons, or operations;
   (b) foreign government information;
   (c) intelligence activities, sources or methods;
   (d) foreign relations or foreign activities of the United States;
   (e) scientific, technological, or economic matters relating to the national security;
   (f) United States Government programs for safeguarding nuclear materials or facilities; or
   (g) other categories of information which are related to national security and which require protection against unauthorized disclosure as determined by the President, by a person designated by the President pursuant to Section 1-201, or by an agency head; and

2. Its unauthorized disclosure could reasonably be expected to cause at least identifiable damage to the national security because of the nature or substance of the information itself or the fact of its possession by the United States Government.

Decisions to exempt a document from declassification must balance the need to safeguard U.S. national security interests against the public's right to know. If classified information or documents from other U.S. Government agencies are found among these records, they will be reviewed under the originating agency's classification review guidelines or be referred to the originating agency for its review as appropriate.

The major concern in the review of the records of the COI, OSS and SSU is to protect sensitive intelligence sources and methods. The Director of the CIA has statutory responsibility to protect intelligence sources and methods.

An intelligence source is a person, organization, group, technical system, mechanism, device or any other means or instrument that has provided or is being developed to provide foreign intelligence or foreign counterintelligence and which, if its identity or capability is disclosed, could be vulnerable to counteraction which may nullify or significantly reduce its effectiveness in providing foreign intelligence or foreign counterintelligence to the United States. The premature disclosure of the identities of sources who cooperated in confidence will undoubtedly have an adverse impact on an intelligence agency's ability to obtain new sources out of the fear of ultimate compromise. Ideally, source identities should never be disclosed but at a minimum they should not be revealed for at least 75 years to afford a basic level of protection to the sources and their immediate families.

A present, past or prospective intelligence method is a procedure, mode, technique, or requirement used or being developed to acquire, transmit, analyze, evaluate, or process foreign intelligence or foreign counterintelligence or which supports an intelligence source or operation and if disclosed, is vulnerable to counteraction that could nullify or significantly reduce its effectiveness in supporting the foreign intelligence or foreign counterintelligence activities of the United States, or could reasonably lead to the disclosure of an intelligence source or operation.

Operational intelligence activities of the COI, OSS, or SSU are not of themselves exempt from declassification, except to the extent that disclosure would expose sensitive intelligence sources or methods currently in use or proposed for use, or do damage to the current or future foreign intelligence or diplomatic interests of the United States.

All classified documents and other materials originated by COI, OSS, or the SSU, or for which they had responsibility, may be declassified except those which, after review under these general guidelines, contain information judged to be still sensitive and which, if declassified, reasonably could be expected to:

1. Identify personnel who were assigned under non-official cover or would reveal a non-official cover arrangement.

2. Security personnel serving under State Department cover in an unusual instance where the situation was politically sensitive because of governmental relationships which still could be adversely affected by disclosure. As a general rule, OSS personnel serving under official cover need not be protected. This applies especially to personnel serving at OSS Headquarters and under military unit cover in the field. Personnel serving in the field under non-military cover, where that cover was a peculiarity of the war-time situation, e.g. Lend Lease, War Shipping Administration (WSA), United States Commercial Corporation (USCC), Office of War Information (OWI), Federal Economic Administration (FEA), and there may have been others, need not be protected.

3. Identify agents informants or collaborators, witting or unwitting, unless already identified in open literature.

4. Reveal the relationship with any element of a cooperating foreign government or international organization, provide details about it, or reveal information obtained in confidence from such an entity. Classified information received from such an entity in confidence may not be declassified without consulting the originating foreign government entity or international organization.

5. Reveal the strategies, procedures, techniques and devices used to acquire, train and employ agents, collaborators and informants, or to create and employ technical sources for intelligence purposes, and which have more than a strictly wartime application.

6. Disclose communication intelligence, cryptography and related activities which must be protected until they can be reviewed by the National Security Agency. An exception to this is German and Japanese encrypted communications intercepted and decoded during World War II which are declassified.

7. Disclose censorship materials which are to be protected until they can be reviewed by the General Services Administration. (See NARS guidelines of 26 April 1978 for exceptions.) Care must be taken to protect any cooperative foreign government or entity of the foreign government which may have been involved in censorship activities.

8. Disclose classified information originated by another U.S. Government agency which should be coordinated with that agency or its successor agency prior to release or be reviewed under the declassification guidelines issued by the originating agency for that purpose.

9. Disclose information which might adversely affect the conduct of current or future U.S. foreign relations.

10. Disclose information which could place a person in jeopardy.

[redacted] STATINTL

Chief,
Classification Review Group
Information Systems Analysis Staff
Directorate of Administration

REVIEW OF FOREIGN GOVERNMENT INFORMATION

1. E.O. 12065 authorizes protection of foreign government information for up to thirty years before requiring it be reviewed for declassification under guidelines developed, where appropriate, in consultation with the foreign government concerned. The Agency position is that classified documents created by a foreign government or foreign government information, however obtained, which is used in OSS reports, may not be declassified without specific instructions from the foreign government concerned. The basis for this position is that such information and documents were given to the U.S. Government with the understanding that they would be held in confidence and, that the unauthorized or inappropriate exposure today could impact adversely on current or future U.S. liaison and diplomatic relations as well as directly on U.S. intelligence equities. These general considerations should be kept in mind when reviewing OSS records, and any given foreign government document or information should be viewed under this light. The basic requirement is to protect current and future CIA and U.S. intelligence interests. Complete guidelines which would neatly cover each and every case presented to the reviewer is not feasible. The following however, are provided to give the reviewer a more specific idea of what requires protection in the areas of sources and methods, liaison relationships, and U.S. foreign relations:

a. Sources and methods - protect the identity of agents and collaborators; informants where a serious and sustained relationship existed; include persons used jointly. Protect intelligence methods, ("theirs," "ours," or "joint") which have had continued applicability in their or our operations or would, if revealed, create a negative reaction from one of our friendly liaison services with whom we continue to cooperate, or could impact adversely on our foreign relations today or in the future. Sensitive intelligence methods are those which are not essentially identical to methods universally employed by intelligence services and therefore widely known, or that have not been rendered obsolete by technological advances.

b. Liaison relationships - consider what the liaison services' attitude and requirements are for release of their own information and records as the basis against which to consider our handling of their documents and information. All services protect their sources and we must do likewise. More difficult to judge is information concerning intelligence methods and organizational data, release of which might cause an adverse reaction that could impact negatively on our current or future relationship with that service. Identification of their personnel is certainly one such category of information that should not be generally released, organizational details another, and information that could reveal something of their methods of operation should receive careful attention.

c. Foreign relations - An even more difficult area in which to render judgments is that information which could impact adversely on current or future U.S. foreign relations. The same categories of information noted above are applicable but here we must consider the additional factor that exposure could impact adversely on current or future U.S. foreign relations. Such problems would likely revolve around prominent personalities, controversial government policies or actions, or government to government relationships considered particularly sensitive and often maintained under some measure of secrecy for that reason. These problems are more likely to arise concerning those countries which were neutral or not totally committed to either side during WW II and who continue to follow somewhat independent roads today. Such countries would be the neutrals such as Sweden, Switzerland, Ireland, Spain and Turkey. While no guide can hope to anticipate all the possibilities let alone cover them, it can at least-or maybe at best-sensitize reviewers to the areas where improper release of information or records could create or contribute to an adverse foreign reaction that would be detrimental to U.S. foreign policies and relations and thus to our national security. The above comments are intended as a general guide, not as a definitive or all inclusive directive. Individual judgment must be relied upon in most cases. When in doubt refer the question to C/CRG/OPS.

2. When you find foreign government information or documents which fall within the above categories they should be treated as any other document and processed as follows:

a. Remove from box and replace with a Withdrawal Notice.
b. Stamp the document with the reviewer's stamp.
c. Fill in the Withdrawal Notice number and the document number from Job No. 79-00332A.

d. Mark to indicate any change in classification.
e. Fill in the year of the "Next Review Date" to indicate a time period of 40 years from the date of the document's creation date (30 years allowed by E.O. 12065 plus 10 years for the first review extension).
f. Fill in the date of the review action and your employee number.
g. Complete Form 4023A as usual.

[redacted]
Chief,
Classification Review Group

STATINTL

2 July 1979

Classification Review Procedure

CRP 79-32 and
CRP 79-008/OSS

GUIDELINES FOR THE REVIEW OF RECORDS FOR THE PERIOD
FROM THE END OF OSS TO THE BEGINNING OF CIA
1 October 1945 - 20 September 1947

BACKGROUND

On 20 September 1945 President Harry Truman signed an Executive Order breaking up the OSS as of 1 October 1945 and directing the Secretary of State to take the lead in developing the program for a comprehensive and coordinated foreign intelligence system. The Research and Analysis (R&A) and Presentation Branches of the OSS went intact to the State Department. The remaining activities of the OSS (mostly clandestine services) were assigned to the War Department which was to keep them separate in the Strategic Services Unit (SSU) established by the Executive Order for that purpose and to keep those activities to serve as a nucleus for a possible central intelligence service.

On 22 January 1946 President Truman issued a Presidential Directive which established the Central Intelligence Group (CIG) functioning directly under the National Intelligence Authority (NIA). The NIA consisted of representatives of the Secretaries of State, War and Navy and a personal representative of the President. The Director of CIG was appointed by the President. His duties included planning to coordinate departmental intelligence activities; recommending policies and objectives of the "national intelligence mission;" correlating and evaluating intelligence for strategic and national policy and disseminating it within the Government; performing functions related to intelligence as the President and NIA might direct; and performing services of common concern where those services could be performed more efficiently by a central organization. Significantly, the Director of CIG was not given the duty of directly collecting intelligence. The CIG was described as "a cooperative interdepartmental activity." Since the SSU had been expected only to serve an interim function, the Executive Order of 20 September 1945 directed the Secretary of War to discontinue the SSU as soon as its functions and facilities could be: 1) placed in a new central intelligence organization; 2) placed in the War Department; or 3) dropped entirely. General Magruder, chief of the SSU, was to superintend the liquidation of those SSU activities to be dropped entirely during peacetime. On 29 January 1946 the Secretary of War directed that the SSU should be liquidated by 30 June 1946. The Director of CIG was to take what records he wanted from SSU through the Secretary of War and retain operational control over them. Title to the records was to be settled later. Magruder felt that SSU plans, properties and personnel must be maintained because they were indispensable for the procurement of intelligence in peacetime. On 14 February 1946 he urged that the SSU be placed under the Director of CIG.

As there was some dispute over whether the Office of CIG should get the entire unit, an interdepartmental committee was organized under Colonel Fortier to study this question. The committee found support for the opinion that the SSU, as was, ought not go to the CIG. The committee had heard that the bulk of intelligence information came from friendly governments; that much material came from other sources than secret collection; that SSU personnel had not been adequately screened; and that many clandestine personnel had become exposed during WW II. The committee thought that the SSU should be reorganized and the desired portion placed under the CIG as a "going concern." The committee thought that CIG should closely coordinate clandestine operations, concentrate on the USSR and the Satellites, penetrate key institutions to aid possible U.S. military operations, develop liaison with foreign intelligence agencies and develop sleeper networks in Germany and Japan while overt collection of intelligence information should remain with the other U.S. Government agencies. The committee also recognized the interrelationship between the SSU and the R&A Branch (still located in the State Department) and urged that their activities be integrated because the R&A Branch was "closely geared to the secret intelligence branches as their chief guide." The committee also felt that the Director of CIG should take authority and responsibility for liquidation of the SSU.

On 3 April 1946 the final liquidation of SSU was postponed from 30 June 1946 to 30 June 1947. Meanwhile, the Chief of SSU was directed to obey the instructions from the Director of CIG. This made it possible for Fortier, Assistant Director and Acting Chief of Operational Services of CIG, to take over such SSU assets as the Director of CIG wanted while unwanted assets would be absorbed into the War Department or abandoned. The arrangements for the transfer of SSU to the CIG through the War Department were complicated but it enabled the CIG to take legally what it wanted while Magruder, Chief of the SSU, got rid of unwanted facilities through the War Department. Although no specific legal action was taken, the passage of time and the inferential approval of the National Security Act of 1947 appears to have vested title of SSU property to the CIG.

In June 1946 General Vandenberg became the Director of CIG (replacing Admiral Souers). Vandenberg felt that the Director of CIG must be the NIA's executive officer and he immediately struck out to obtain greater authority and independence for the CIG. While his ideas met resistance from the member agencies of NIA, Vandenberg did win some points. For example, Vandenberg wanted the CIG to conduct all espionage and counter-espionage for the collection of foreign intelligence abroad. This proposal was modified to allow the Director of CIG to conduct only those "organized federal" operations which were outside the U.S. and its possessions, but still left CIG with the authority to collect intelligence information. The purpose of the revision was to permit the military services to collect intelligence for departmental purposes and it was meant to protect the FBI in performing its duties within the U.S. Vandenberg then established the Office of Special Operations to collect foreign intelligence. During the summer and fall of 1946, the CIG arranged to take over the personnel, undercover agents, and foreign stations of the SSU. By mid-October 1946 the liquidation of SSU was complete. (SSU as a bonafide organization never actually went out of business. The C/IMS/DDO is the current chief of SSU and is authorized to conduct certain business for

and on behalf of SSU. Most SSU activities involve checking out special requests from EX-SSU or OSS personnel.) Field stations were notified that effective 19 October 1946 "SSU discontinues all overseas activities and the Office of Special Operations of CIG assumes responsibility for conducting espionage and counterespionage in the field for collection of foreign intelligence information required for national security."

As noted above, the CIG takeover of the SSU stretched over a period of several months in 1946. During this period the CIG took over many of the personnel, installations, facilities and cover arrangements and units as well as administrative practices of the SSU. Thus you will find CIG, after 19 October 1946, using SSU cover unit designations and letterhead stationery from such units making it difficult to identify CIG documents from appearance alone. It could be argued that if the letterhead is SSU then it is an SSU document. Be that as it may, for general purposes in classification review consider all records created before 19 October 1946 as SSU and all records created after that date as CIG.

GUIDELINES

For our general use in the classification review process, the date of 19 October 1946 will be considered the pivotal date marking the "end" of the SSU and the "beginning" of the CIG. Generally speaking, records dated prior to 19 October 1946 will be considered SSU documents and those created after that date will be considered CIG documents.

The methods of organization and operation used by the SSU were very similar to those developed and used by the OSS. The SSU was essentially a military unit, staffed mostly by military personnel and housed in the War Department under military command. It is therefore pertinent for us to review SSU documents under those guidelines developed for and used in the classification review of OSS records. The CIG on the other hand, very soon after its creation began to take on an independent life and although many CIG personnel continued to be military it quickly attracted more civilians and it was not under direct military command. We will, therefore, look at CIG documents as relating closely to the beginnings of the CIA and will review CIG documents under those guidelines developed for and used in the classification review of CIA records. As a general rule, the OSS review team will be responsible for reviewing documents originated before 19 October 1946 and the other CRD reviewers will be responsible for those documents originated after 19 October 1946. This date is not intended to be an absolute rule; as in all review work, individual judgement must be used. For example, a document originated after 19 October 1946 might refer to the past and to activities or problems of the SSU making it in essence a more or less typical SSU document containing material relating to the SSU. Such a document should be reviewed as being essentially a SSU document and using the OSS guidelines to judge the classification action. On the other hand, a document originated before 19 October 1946 might refer to the future and to activities or problems relating to the CIG making it in essence a more or less typical CIG document. This type document should be reviewed as a CIG document using the CIA guidelines.

All reviewers should be especially alert for these types of documents and pay particular attention to their classification review. If there is any question, coordination should be effected between the CRD Operations Branch/OSS and the CRD Operations Branch/CIA through the Chief of the CRD Operations Branch.

The major categories of information which most likely will require continued protection are: 1) information which identifies sources; 2) foreign government information and details of intelligence agreements we had with foreign governments; 3) information revealing unique intelligence methods not generally known or used and not outdated; and 4) information which could still cause negative reactions that could impact adversely on current or future U.S. foreign relations. Some more specific guidelines are as follows:

1. Protect all sources to avoid creation of a reputation that U.S. intelligence services cannot protect their sources. A rare exception to this rule might be possible where the contact was fleeting, incidental, insignificant and overt.

2. Identification as an SSU staffer will be judged and handled the same way as it is for an OSS staffer. Staffers generally will not be protected merely because they later worked for the CIG or the CIA. If however, the person engaged in sensitive work for CIG or the CIA, their SSU (and OSS) employment may be exempted from declassification to protect the later sensitive work or position in the CIG or the CIA.

3. Persons who served under non official cover are protected at all times as is their cover.

[redacted] STATINTL

Chief,
Classification Review Division

The Director
Central Intelligence Agency

Washington, D.C. 20505

5 JUN 1979

Mr. Michael T. Blouin
Director, Information Security Oversight Office
General Services Administration
Washington, D.C. 20405

Dear Mr. Blouin:

Enclosed for your review are guidelines issued pursuant to Executive Order 12065 for the systematic review of United States originated classified information over twenty years old and under Central Intelligence Agency classification jurisdiction. Also enclosed is a copy of my letter to the Archivist of the United States forwarding these guidelines for his use.

Yours sincerely,

STANSFIELD TURNER

Enclosures

Approved For Release 2002/02/14 : CIA-RDP85B00236R000100170009-7

The Director
Central Intelligence Agency

Washington, D.C. 20505

5 JUN 1979

Dr. James B. Rhoads
Archivist of the United States
National Archives and Records Service
Eighth Street and Pennsylvania Avenue, N.W.
Washington, D.C. 20408

Dear Dr. Rhoads:

Pursuant to Section 3-402 of Executive Order 12065, I hereby issue and enclose for your use the required systematic review guidelines covering classified information of United States origin and more than twenty years old over which the Central Intelligence Agency has classification jurisdiction. These guidelines were prepared in consultation with your designated representative Mr. Edwin A. Thompson, Director of the Records Declassification Division, National Archives and Records Service.

Copies of this letter and of the enclosed guidelines have been forwarded to the Director of the Information Security Oversight Office (ISOO) for his review, as provided by the Order. Systematic review guidelines for "foreign government information" as defined in Section 6-103 of the Order and in Section I/F of ISOO Directive No. 1 will be provided at a later date, in compliance with the provisions of the Order and Directive concerning such information.

Yours sincerely,

STANSFIELD TURNER

Enclosure

CENTRAL INTELLIGENCE AGENCY

SYSTEMATIC REVIEW GUIDELINES

A. Authorization. The following guidelines apply to information of United States origin which is more than 20 years old and over which the Central Intelligence Agency has classification jurisdiction. Under the provisions of Section 3-402 of Executive Order 12065, the CIA authorizes the Archivist of the United States to use these guidelines in the review of such information upon its transfer to the General Services Administration and accession into the National Archives.

B. Categories of Information Excepted from Automatic Declassification. Except for foreign government information, which is exempt from automatic declassification under Section 3-404 of the Order, all classified information over 20 years old which is under the classification jurisdiction of this agency is automatically declassified unless it falls within one or more of the categories described below. Information in these categories shall not be declassified until reviewed for declassification by designated CIA personnel, and must be referred to CIA for such review by all other agencies having custody thereof. Waiver of the Order's 10-year review interval requirement having been granted pursuant to Section 3-401 by the Director of the Information Security Oversight Office, information in Categories 1 through 5 below is to be systematically reviewed again 30 years following its initial review. Information in all other categories listed below shall be re-reviewed at 10-year intervals, as necessary, until it can be declassified or assigned a date or event for automatic declassification. Category 29 is a new category under Section 1-301(g) of the Order.

CATEGORY 1

Information constituting or concerning cryptologic, cryptographic or signals intelligence including information on the development and/or use of any method, means, system, device, installation or activity for the production, acquisition or transmission of such intelligence or for the protection of cryptographically processed data including cryptographic, communications and emanations security procedures, techniques, materials and equipment.

(Next Review Date: 30 years following initial review.)

CATEGORY 2

Information constituting or concerning counterintelligence, defined by Executive Order 12036 of 24 January 1978 (Section 4-202) as "...information gathered and activities conducted to protect against espionage and other

clandestine intelligence activities, sabotage, international terrorist activities or assassinations conducted for or on behalf of foreign powers, organizations or persons, but not including personnel, physical, document or communications security programs."

(Next Review Date: 30 years following initial review.)

CATEGORY 3

Information concerning or covered by special access, distribution and protection programs continued or established pursuant to Section 4-2 of Executive Order 12065.

(Next Review Date: 30 years following initial review.)

CATEGORY 4

Information which identifies any undercover personnel or unit(s), or clandestine human agent(s), of the Central Intelligence Agency or of a predecessor agency; or which otherwise reveals information classifiable under the provisions of Executive Order 12065 concerning intelligence sources, methods or activities including intelligence plans, policies, or operations of the Central Intelligence Agency, a predecessor agency, or any element of either.

(Next Review Date: 30 years following initial review.)

CATEGORY 5

Information covertly acquired which is contained in intelligence reports and other documents that bear the legend "THIS IS UNEVALUATED INFORMATION" or, lacking this or an equivalent marking, are similar in format or content to items so marked; and in which the formats used, subject matter, source descriptions or other content would, in collections or aggregates of such reports and/or other documents, reveal the nature, scope or extent of United States intelligence activities in, or in relation to, particular foreign countries or areas or would identify intelligence sources or methods.

(Next Review Date: 30 years following initial review.)

CATEGORY 6

Information which reveals or identifies a present, past, or prospective intelligence source, whether a person, organization, group, technical

system, mechanism, device, or any other means or instrument that provides, has provided, or is being developed to provide intelligence.

CATEGORY 7

Information which reveals or identifies a present, past, or prospective intelligence method, procedure, mode, technique, or requirement used or being developed to acquire, transmit, analyze, correlate, evaluate, or process intelligence or to support an intelligence source, operation, or activity.

CATEGORY 8

Information that discloses the organizational structure of the Central Intelligence Agency; the numbers and assignments of CIA personnel; the size and composition of the CIA budget, including internal and external funding; logistical and associated support activities and services; security procedures, techniques, and activities including those applicable to the fields of communications and data processing; or other quantitative or qualitative data revealing or indicating the nature, objectives, requirements, priorities, scope or thrust of CIA activities, including the missions, functions, and locations of certain CIA components or installations.

CATEGORY 9

Information pertaining to intelligence-related methodologies, techniques, formulae, equipment, programs or models, including computer simulations, ranging from initial requirements through planning, source acquisition, contract initiation, research, design, and testing to production, personnel training, and operational use.

CATEGORY 10

Information which identifies research, procedures, or data used by CIA in the acquisition and processing of intelligence or the production of finished intelligence, when such identification could reveal the particular intelligence interest of the CIA, the value of the intelligence, or the extent of the CIA's knowledge of a particular subject of intelligence interest.

CATEGORY 11

Information pertaining to training in intelligence sources, methods, and activities provided under the auspices of CIA to individuals, organizations, or groups that could reveal or identify equipment, materials, training sites, methods and techniques of instruction, or the identities of students and instructors.

CATEGORY 12

Information that could disclose CIA policies and procedures used for personnel recruitment, assessment, selection, training, assignment, and evaluation.

CATEGORY 13

Information that could lead to foreign political, economic, or military action against the United States or other friendly nations.

CATEGORY 14

Information that could create, stimulate, or increase international tensions in such manner as to impair the conduct of United States foreign policies.

CATEGORY 15

Information that could deprive the United States of a diplomatic or economic advantage related to the national security, or that could weaken the position of the United States or its allies in international negotiations, or adversely affect other activities pertinent to the resolution or avoidance of international conflicts or differences having national security significance.

CATEGORY 16

Information concerning plans prepared, under preparation, or contemplated by officials of the United States to meet diplomatic or other contingencies affecting the national security.

CATEGORY 17

Information that identifies or otherwise reveals activities conducted abroad in support of national foreign policy objectives, and planned and executed so that the role of the United States Government is not apparent or acknowledged publicly; or information that discloses support provided to such activities.

CATEGORY 18

Information revealing that the United States has obtained, or seeks to obtain, certain data or materials from or concerning a foreign nation, organization, or group; the disclosure of which information could adversely affect United States relations with or activities in a foreign country.

CATEGORY 19

Information that could lead to political or economic instability, or to civil disorder or unrest, in a foreign country or jeopardize the lives, liberty, or property of United States persons in such a country or could endanger United States Government personnel or installations there.

CATEGORY 20

Information concerning foreign intentions, capabilities, or activities which could pose a potential threat to United States national security interests or to those of allied or other friendly governments.

CATEGORY 21

Information indicating the extent of, or degree of success achieved by, United States collection of intelligence on and assessment of foreign military plans, weapons, capabilities, or operations.

CATEGORY 22

Information revealing defense plans or posture of the United States, its allies, or other friendly countries or enabling a foreign nation or entity to develop countermeasures to such plans or posture.

CATEGORY 23

Information disclosing the capabilities, vulnerabilities, or deployment of United States weapons or weapons systems.

CATEGORY 24

Information that continues to provide the United States with a scientific, technical, engineering, economic, or intelligence advantage of value to the national security.

CATEGORY 25

Information concerning research of a scientific or technical nature leading to the development of special techniques, procedures, equipment and equipment configurations, systems, or devices for collection or production of foreign intelligence; or the operational planning for, deployment or use thereof in such collection or production, or for other national security purposes.

CATEGORY 26

Information concerning United States Government programs to safeguard nuclear materials, techniques, capabilities, or facilities that could compromise, jeopardize or reduce the effectiveness of such programs.

CATEGORY 27

Information on foreign nuclear programs, activities, capabilities, technologies, facilities, plans and intentions, weapons and their deployment that could disclose the nature, scope, or effectiveness of United States intelligence efforts to monitor nuclear developments abroad or could cause such efforts to fail or be restricted in a manner detrimental to national security.

CATEGORY 28

Information pertaining to contractual relationships or joint arrangements with individuals, commercial concerns or other entities when such a relationship or arrangement involves a specific intelligence interest, or reveals the extent or depth of knowledge or technical expertise possessed by CIA, or when disclosure of the relationship or arrangements could jeopardize the other party's willingness or ability to provide services to CIA.

CATEGORY 29

Information that could result in or lead to action(s) placing an individual in jeopardy.

C. Agency Assistance to the National Archives. This agency has designated experienced personnel to guide and assist National Archives personnel in identifying and separating documents and specific elements of information within documents under these categories that are deemed to require continued protection. These CIA-designated personnel are authorized to declassify categories of information exempted from automatic declassification (listed in the preceding section) if it is determined that they no longer require protection. These CIA personnel will make recommendations for continued classification of the documents or categories of information requiring continued protection.

D. Continuing Application of Earlier Guidelines. The systematic review guidelines and instructions identified below shall remain in effect until canceled or superseded:

1. Downgrading instructions provided in the letter of 16 April 1973 from Lawrence R. Houston, Central Intelligence Agency General Counsel, to Dr. James B. Rhoads, Archivist of the United States.

2. Instructions concerning information on Secret Writing (S/W), cited in the letter of 8 June 1973 from [redacted] Central Intelligence Agency Archivist, to Mr. Edwin A. Thompson, Director of the Records Declassification Division, National Archives and Records Service. STATINTL

STATINTL

3. Guidelines concerning [redacted] material, cited in the letter of 23 August 1977 to Mr. Edwin A. Thompson, Director of the Records Declassification Service, National Archives and Records Service, from [redacted] Central Intelligence Agency Senior Review Officer.

STATINTL

4. Central Intelligence Agency issuance dated 11 December 1978 and entitled "GUIDELINES FOR CLASSIFICATION REVIEW OF CIA PREDECESSOR RECORDS AND INFORMATION BETWEEN 1941-1946", signed by [redacted] Chief of the Classification Review Group, Information Systems Analysis Staff, Directorate of Administration.

STATINTL

STANSFIELD TURNER

The Director
Central Intelligence Agency

Washington, D.C. 20505

10 JAN 1980

Mr. Robert W. Wells
Acting Director, Information Security Oversight Office
General Services Administration
Washington, D.C. 20405

Dear Mr. Wells:

CIA concurs in the Guidelines for Systematic Review of Foreign Government Information Thirty Years Old or Older forwarded under Director, Information Security Oversight Office letter of 11 December 1979.

STANSFIELD TURNER

General Services Administration
Information Security Oversight Office
Washington, DC 20405

Admiral Stansfield Turner, USN
Director
Central Intelligence Agency
Washington, DC 20505

Dear Admiral Turner:

Enclosed is the final draft of the Foreign Government Information Guidelines agreed upon after months of consultation by a working group of senior officials from all affected agencies. They are being forwarded to you for your final and official review.

Please notify this office within 30 days of your official concurrence with the enclosed. Many thanks for your assistance in the development of this product.

Kindest regards,

Sincerely,

MICHAEL T. BLOUIN
Director

Enclosure

GUIDELINES FOR SYSTEMATIC REVIEW OF FOREIGN GOVERNMENT INFORMATION THIRTY YEARS OLD OR OLDER

A. PURPOSE.

These Guidelines for the systematic review and declassification of foreign government information have been developed in accordance with the provisions of Section 3-404 of Executive Order 12065, "National Security Information," and Section III.C of Information Security Oversight Office Directive No. 1. All foreign government information constituting permanently valuable records of the United States Government, for which a prior declassification date has not been established, shall be systematically reviewed for declassification as it becomes thirty years old. Foreign government information found to be within one of the specific categories of information listed in Part F below shall be reviewed item-by-item by authorized personnel of the agency or agencies concerned to determine whether continued protection beyond thirty years is needed. All foreign government information not identified in these Guidelines as requiring item-by-item review and for which a prior declassification date has not been established shall be declassified at the end of thirty years from the date of original classification subject, when appropriate, to consultation with the foreign governments or international organizations of governments concerned.

B. DEFINITION.

"Foreign government information" as used in these Guidelines consists of:

1. Documents or material provided by a foreign government or governments, international organization of governments, or any element thereof in the expectation, expressed or implied, that the document, material, or the information contained therein is to be held in confidence;

2. Documents originated by the United States that contain classified information provided, in any manner, to the United States by foreign governments, international organizations of governments, or elements thereof, with the expectation, express or implied, that the information will be held in confidence;

3. Classified information or material produced by the United States pursuant to or as a result of a joint arrangement, evidenced by an exchange of letters, memorandum of understanding, or other written record, with a foreign government or organization of governments requiring that the information, the arrangement, or both be kept in confidence.

C. SCOPE.

1. These Guidelines apply to 30-year old foreign government information which has been received or classified by the United States Government or its agents.

2. Atomic energy information (including that originated prior to 1947 and not marked as such, that received from the United Kingdom or Canada marked "Atomic," and that received from NATO marked "Atomal") which is defined and identified as Restricted Data or Formerly Restricted Data in Sections 11y and 142d of the Atomic Energy Act of 1954, as amended, is outside the scope of these Guidelines and is not subject to systematic review and may not be automatically downgraded or declassified. Any document containing information within the definition of Restricted Data or Formerly Restricted Data that is not so marked will be referred to the Department of Energy Office of Classification for review and appropriate marking, except for licensing and related regulatory matters which shall be referred to the Division of Security, U.S. Nuclear Regulatory Commission.

D. AGENCY RESPONSIBILITIES.

1. Foreign government information transferred to the General Services Administration for accession into the National Archives of the United States shall be reviewed for declassification by the Archivist of the United States in accordance with Executive Order 12065, the directives of the Information Security Oversight Office, these Guidelines, any applicable terms of accession, and any supplemental guidelines provided by the agency with classification jurisdiction over the information.

2. Foreign government information constituting permanently valuable records of the Government (as defined in 44 U.S.C. 2103) that is 30 years old and undergoing systematic review for declassification while in the custody of an agency shall, except as provided in Part C, above, be reviewed for declassification and downgrading by that agency in accordance with Executive Order 12065, the directives of the Information Security Oversight Office, these Guidelines, and any supplemental internal agency guidelines.

3. Foreign government information falling within any of the categories listed in Part F of these Guidelines shall be declassified or downgraded only upon specific authorization of the agencies to which the information was furnished by the foreign government or international organization of governments concerned and/or which have classification jurisdiction over it. When such information is in the custody of an agency but was furnished to or classified by, or is otherwise under the classification jurisdiction of another agency or agencies the information shall be referred thereto for review. Information so referred shall remain classified until all reviewing agencies have authorized its declassification. If the custodial agency cannot readily identify the agency or agencies having classification jurisdiction, the information shall be referred in accordance with Part G of these Guidelines for review or further referral.

4. Foreign government information falling within any of the categories listed in Part F of these Guidelines appearing in White House documents, which is either identifiable as having been furnished or appears to have been furnished by a foreign government shall be reviewed by designated White House personnel and further referred for review to any other agencies whose classification interest is indicated by the nature or content of the documents.

E. EFFECT OF PUBLICATION.

1. Foreign government information is declassified if already published in or cleared by executive branch officials authorized to declassify the information, and/or by the foreign government(s) involved, as appropriate, for publication in any unclassified executive branch publication; or if officially published as unclassified by the foreign government or international organization of governments that furnished the information, unless the fact of the U.S. Government's possession of the information requires continued protection.

2. The unofficial publication, in any manner, of foreign government information contained in United States or foreign documents, or of substantially similar information, does not in or of itself constitute or permit the declassification of such documents. The original sources of the information, or the means whereby it was acquired by the United States Government, may require continued protection and could preclude declassification. Nevertheless, unofficial publication is a factor to be considered in the systematic review of information and may affect determinations as to requirements for its continued classification protection. However, the classification status of information which concerns or derives from intelligence activities, sources or methods shall not be affected by any unofficial publication of similar or identical information. Final determinations as to the declassification of information identical with or similar to unofficially published information shall be made by the agency or agencies holding classification jurisdiction over the information.

F. CATEGORIES REQUIRING ITEM-BY-ITEM REVIEW.

Foreign government information falling into the specific categories listed below shall be reviewed for declassification in accordance with Part A above:

1. Information exempted from declassification under any joint arrangement evidenced by an exchange of letters, memorandum of understanding, or other written record, with the foreign government or international organization of governments, or element(s) thereof, that furnished the information. Questions concerning the existence or applicability of such arrangements shall be referred to the agency or agencies holding classification jurisdiction over the records under review.

2. Information related to the safeguarding of nuclear materials or facilities, foreign and domestic, including but not necessarily limited to vulnerabilities and vulnerability assessments of nuclear facilities and Special Nuclear Material.

3. Nuclear arms control information (see also #11 below).

4. Information regarding foreign nuclear programs (other than Restricted Data and Formerly Restricted Data), such as:

a. Nuclear weapons testing.
b. Nuclear weapons storage and stockpile.
c. Nuclear weapons effects, hardness, and vulnerability.
d. Nuclear weapons safety.
e. Cooperation in nuclear programs including, but not limited to, peaceful and military applications of nuclear energy.
f. Exploration, production and import of uranium and thorium from foreign countries.

5. Information concerning intelligence or counterintelligence sources, methods or activities including but not limited to intelligence, counterintelligence and covert action programs, plans, policies, operations, or assessments; or which would reveal or identify:

a. Any present, past or prospective undercover personnel, installation, unit, or clandestine human agent, of the United States or of a foreign government;
b. Any present, past or prospective method, procedure, mode, technique or requirement used or being developed by the United States or by foreign governments, individually or in combination, to produce, acquire, transmit, analyze, correlate, assess, evaluate or process intelligence or counterintelligence, or to support an intelligence or counterintelligence source, operation, or activity;
c. The present, past or proposed existence of any joint United States and foreign government intelligence, counterintelligence, or covert action activity or facility, or the nature thereof.

6. Information that could result in or lead to actions which would place an individual in jeopardy directly attributable to disclosure of the information, including but not limited to:

a. Information identifying any individual or organization as a confidential source of intelligence or counterintelligence.
b. Information revealing the identity of an intelligence, counter-intelligence or covert action agent or agents.

7. Information about foreign individuals, organizations or events which, if disclosed, could be expected to:

a. Adversely affect a foreign country's or international organization's relations with the United States.
b. Adversely affect present and/or future confidential exchanges between the United States and any foreign government or international organization of governments.

8. Information related to plans (whether executed or not, whether presented in whole or in part), programs, operations, negotiations, and assessments shared by one or several foreign governments with the United States, including but not limited to those involving the territory, political regime or government of another country, and which if disclosed could be expected to adversely affect the conduct of U.S. foreign policy or the conduct of another country's foreign policy with respect to a third country or countries. This item would include contingency plans, plans for covert political, military or paramilitary activities or operations by a foreign government acting alone or jointly with the United States Government, and positions or actions taken by a foreign government alone or jointly with the United States concerning border disputes or other territorial issues.

9. Information concerning arrangements with respect to foreign basing of cryptologic operations and/or foreign policy considerations relating thereto.

10. Scientific information such as that concerning space, climatology, communications, maritime, undersea, and polar projects, that could be expected to adversely affect current and/or future exchanges of such information between the United States and any foreign governments or international organizations of governments.

11. Information on foreign policy aspects of nuclear matters, the disclosure of which could be expected to adversely affect cooperation between one or more foreign governments and the United States Government.

12. Nuclear propulsion information.

13. Information concerning the establishment, operation, and support of nuclear detection systems.

14. Information concerning or revealing military or paramilitary escape, evasion, cover or deception plans, procedures, and techniques whether executed or not.

15. Information which could adversely affect the current or future usefulness of military or defense policies, programs, weapon systems, operations, or plans.

16. Information concerning research, development, testing and evaluation of chemical and biological weapons and defense systems; specific identification of chemical and biological agents and munitions; and chemical and biological warfare plans.

17. Technical information concerning weapons systems and military equipment that reveals the capabilities, limitations, or vulnerabilities of such systems or equipment and that could be exploited to destroy, counter, render ineffective or neutralize such weapons or equipment.

18. Cryptologic information, including cryptologic sources and methods, currently in use. This includes information concerning or revealing the processes, techniques, operations, and scope of signal intelligence comprising communications intelligence, electronics intelligence, and telemetry intelligence, the cryptosecurity and emission security components of communications security, and the communications portion of cover and deception plans.

19. Information concerning electronic intelligence, telemetry intelligence and electronic warfare (electronic warfare support measures, electronic counter-countermeasures or related activities, including but not necessarily limited to:

a. Nomenclature, functions, technical characteristics or descriptions of communications and electronic equipment, its employment/development, and its association with weapon systems or military operations.
b. The processes, techniques, operations or scope of activities involved in the acquisition, analysis and evaluation of such information, and the degree of success achieved by the above processes, techniques, operations or activities.

20. Present, past or proposed protective intelligence information relating to the sources, plans, techniques, equipment and methods in carrying out assigned duties of protecting United States Government officials or other protectees abroad and foreign officials while in the United States or United States possessions. This includes information concerning the identification of witnesses, informants and persons suspected of being dangerous to persons under protection.

21. Information on deposits of foreign official institutions in United States banks and on foreign official institutions' holdings, purchases and sales of long-term marketable securities in the United States.

22. Information concerning economic and policy studies and sensitive assessments or analyses of economic conditions, policies or activities of foreign countries or international organizations of governments received through the Multilateral Development Banks or through the International Monetary Fund (IMF) and the Organization for Economic Cooperation and Development (OECD).

23. Information described in subparts 2-22 of this Part contained in correspondence, transcripts, memoranda of coversation, or minutes of meetings between the President of the United States and a current or former foreign government official.

24. Information described in subparts 2-22 of this Part contained in documents originated by or sent to the Assistant to the President for National Security Affairs, his Deputy, members of the National Security Council staff, or any other person performing national security functions on behalf of the White House.

25. Federal agency originated documents bearing NSC or White House comments relating to categories of information described in subparts 2-22 of this Part.

26. Information as described in subparts 2-22 of this Part contained in correspondence to or from the President, including background briefing memoranda and talking points for meetings between the President and foreign government officials, and discussions of the timing and purposes of such meetings.

27. Information as described in subparts 2-22 of this Part contained in agency message traffic originated by White House Staff members but sent through agency communication networks.

G. REFERRAL AND DECISION.

1. When the identity of agencies holding classification jurisdiction over foreign government information is not apparent upon initial inspection, or when reviewing officials do not possess the requisite expertise, the information shall be referred as follows to an agency competent to make the decisions required or further to refer the information for review by the appropriate agency or agencies:

Categories	2 - 4,	Department of Energy or Nuclear Regulatory Commission (as appropriate)
	5 - 6,	Central Intelligence Agency
	7 - 11,	Department of State
	12 - 19,	Department of Defense
	20 - 22,	Department of the Treasury
	23 - 27,	National Security Council

2. When agencies have determined on their own authority, and/or after consultation when necessary with other U.S. agencies and with foreign governments or international organization of governments which furnished the information as appropriate, that information under their jurisdiction no longer requires classification protection, such information shall then be declassified. Such action may involve the declassification of an entire document, or only portions of a document. If it is determined that classification must be extended beyond 30 years, the provisions of Section III,C,2(b) of Information Security Oversight Office Directive No. 1 apply.

H. DOWNGRADING.

Foreign government information classified Top Secret may be downgraded to Secret after 30 years unless an agency with classification jurisdiction over it determines on its own authority, or after consultation, as appropriate, with the foreign government or international organization of governments which furnished the information, that it requires continued protection at the Top Secret level.

General Services Administration
Information Security Oversight Office
Washington, DC 20405

14 JAN 1980

Admiral Stansfield Turner, USN
Director
Central Intelligence Agency
Washington, DC 20505

Dear Admiral Turner:

Section 3-403 of Executive Order 12065, "National Security Information," authorizes the Secretary of Defense to establish special procedures for the systematic review and declassification of classified cryptologic information. Further, Section III.C.2.d. of Information Security Oversight Office Directive No. 1 provides that such procedures promulgated in accordance with the provisions of Section 3-403 of the Order shall be binding on all departments and agencies.

By enclosure to our letter of October 4, 1979, we distributed to you a copy of such procedures. The document entitled, "Special Procedures for Use in Systematic Review of Cryptologic Information Pursuant to Section 3-403 of Executive Order 12065," bears a National Security Agency letterhead and is dated September 1979.

Attached herewith is a copy of revised procedures dated January 1980 which supersede the ones mentioned above. Please insure that all appropriate personnel/activities are furnished copies of the revision and that, where possible, all superseded copies be destroyed.

Sincerely,

Robert W. Wells

ROBERT W. WELLS
Acting Director

Enclosure

OFFICE OF THE UNDER SECRETARY OF DEFENSE
WASHINGTON, D.C. 20301

POLICY

January 1980

SPECIAL PROCEDURES FOR USE IN SYSTEMATIC REVIEW OF CRYPTOLOGIC INFORMATION PURSUANT TO SECTION 3-403 OF EXECUTIVE ORDER 12065

1. General guideline: cryptologic information uncovered in systematic review for declassification of 20/30 year old government records is not to be declassified by other than U.S. government cryptologic agencies. The information may concern or reveal the processes, techniques, operations, and scope of signals intelligence comprising communications intelligence, electronics intelligence, and telemetry intelligence, or it may concern the cryptosecurity and emission security components of communications security, including the communications portion of cover and deception plans.

2. Recognition of cryptologic information may not always be an easy task. There are several broad classes of cryptologic information, as follows:

a. Those that relate to communications security (COMSEC). In documentary form, they provide COMSEC guidance or information. Normally, COMSEC documents and materials are accountable under the "Communications Security Material Control System." Examples are: items bearing "TSEC" nomenclature ("TSEC" plus three letters), "Crypto Keying Material" for use in enciphering communications, Controlled COMSEC Items (CCI), and cryptographic keying devices.

b. Those that relate to signals intelligence (SIGINT). These appear as reports in various formats that bear security classification, sometimes followed by a five-letter codeword (World War II's ULTRA, for example) and often carry warning caveats such as "This document contains codeword material," "Utmost secrecy is necessary . . . ." Formats will appear, for example, as messages having addresses, "from" and "to" sections, and as summaries with SIGINT content with or without other kinds of intelligence and comment.

c. Research, development, test, and evaluation reports and information that relates to either COMSEC or SIGINT.

3. Commonly used words that may help in identification of these documents and materials are "cipher," "code," "codeword," "communications intelligence" or "COMINT," "communications security" or "COMSEC," "cryptanalysis," "crypto," "cryptography," "cryptosystem," "decipher," "decode," "decrypt," "direction finding," "electronic intelligence" or "ELINT," "electronic security," "encipher," "encode," "encrypt," "intercept," "key book," "signals intelligence" or "SIGINT," "signal security," and "TEMPEST."

4. Special procedures apply to the review and declassification of classified cryptologic information. The following shall be observed in the review of such information:

a. COMSEC Documents and Materials. If records or materials in this category are found in agency or department files that are not under COMSEC control, refer them to the senior COMSEC authority of the agency or department concerned or by appropriate channels to the following address:

Director, National Security Agency/
Chief, Central Security Service
ATTN: Policy Staff
Fort George G. Meade, MD 20755

b. SIGINT Information.

(1) If the SIGINT information is contained in a document or record originated by a U. S. government cryptologic organization and is in the files of a non-cryptologic agency or department, such material will not be declassified. The material may be destroyed unless the holding agency's approved records disposition schedule requires its retention. If the material must be retained, it must be referred to the originating organization for systematic review for declassification.

(2) If the SIGINT information has been incorporated by the receiving agency or department into documents it produces, referral of the SIGINT information to the originator is necessary prior to any declassification action.

General Services Administration

Information Security Oversight Office

Washington, DC 20405

DD/A Registry
79-3152

Reply to Attn of: Director, Information Security Oversight Office

Subject: Waiver for 10-year review requirement

To: Senior Officials
All Executive Branch Agencies

By the provisions of Section 3-401, Executive Order 12065, the Director of the Information Security Oversight Office is given the authority to extend the period between subsequent reviews for declassification for specific categories of documents or information.

In response to requests for waivers of the 10-year review requirement from agencies of the executive branch, this Office made the decision that, rather than granting a series of waivers from various agencies of the executive branch covering their own particular fields of interest, a single waiver should be granted that would be applicable and responsive to the needs of all executive branch agencies. This approach was taken to promote uniformity throughout the executive branch information security program.

In developing this waiver, extensive coordination was conducted with the major classifying agencies such as the Central Intelligence Agency, and the Departments of State, Defense, Justice and Treasury. The enclosed waiver reflects the views of those agencies. The efforts to develop the final version of the waiver were greatly facilitated by the personal interest and involvement of Admiral Turner, Director of Central Intelligence.

It is requested that the provisions of the enclosed waiver be brought to the immediate attention of all officials within your agencies. Any extension of the period for subsequent declassification reviews for material covered by the waiver shall be accomplished strictly in accordance with the enclosed procedures.

Thank you for your assistance in this matter.

MICHAEL T. BLOUIN
Director

Enclosure

CATEGORIES OF INFORMATION FOR WHICH THE DIRECTOR OF THE INFORMATION SECURITY OVERSIGHT OFFICE (ISOO) HAS GRANTED WAIVERS OF THE 10-YEAR REVIEW REQUIREMENT OF SECTION 3-401 OF EXECUTIVE ORDER 12065

The Director of the Information Security Oversight Office has granted a waiver from the 10-year review requirements prescribed in Section 3-401 of Executive Order 12065 for the following categories of information:

-- Intelligence documents and/or material(s) constituting or containing identifiable foreign government information as defined in Section 6-103 of Executive Order 12065 and Section I F.1 of Information Security Oversight Office Directive No. 1.

-- Information constituting or concerning cryptology, including information on the development and/or use of any method, means, system, technique, procedure, activity, installation, device, material or equipment used for the acquisition, production, or transmission of signals intelligence or for the protection of classified communications or data."

-- Information constituting or concerning counterintelligence, defined by Executive Order 12036 of January 24, 1978 (section 4-202) as "... information gathered and activities conducted to protect against espionage and other clandestine intelligence activities, sabotage, international terrorist activities or assassinations conducted for or on behalf of foreign powers, organizations or persons, but not including personnel, physical, document, or communications security programs."

-- Information involving or concerning intelligence sources and methods and covered under special access, distribution and protection programs continued or established pursuant to Section 4-2 of Executive Order 12065.

-- Information which identifies any undercover personnel or unit(s) or clandestine human agent(s) of a National Foreign Intelligence Board or other United States Intelligence Community member agency; or which otherwise reveals information classifiable under the provisions of Executive Order 12065 concerning intelligenc sources, methods or activities including intelligence plans, policies, or operations of such an agency or any element thereof.

-- Intelligence reports and other documents which contain information covertly acquired and which bear the legend, "THIS IS UNEVALUATED INFORMATION" or an equivalent marking, or are similar in format or contents to items so marked; and in which the formats used, subject matter, source descriptions or other content would, in collections or aggregates of such reports and/or other documents, reveal the nature, scope or extent of United States intelligence activitie in, or in relation to, particular foreign countries or areas or would identify intelligence sources or methods.

The application of the 10-year review waiver shall be strictly limited to information described above that:

-- has been systematically reviewed following its 20th anniversary, or its 30th anniversary in the case of foreign government information;

-- is identified through such review as requiring continued classification for a period in excess of twenty additional years;

-- cannot, when so reviewed, be assigned a definitive date or event for declassification, thus requiring at least one additional review; and,

-- has its classification extended beyond 20 years, or 30 years in the case of foreign government information, by an agency head or official designated by the President as authorized to do so under Executive Order 12065.

Information to which this waiver is applied shall be re-reviewed 30 years after its initial systematic review, and thereafter at 10-year intervals if necessary.

This waiver applies only to the systematic review process prescribed in Section 3-401 of Executive Order 12065. Information requested under the Freedom of Information Act or the mandatory review provisions of Executive Order 12065 will continue to be processed in accordance with the Act and the Order, whether or not the information falls within the categories of information for which this waiver is granted; nor shall this waiver be construed as an exemption from any requirements imposed on an agency by Section 3-303 of E.O. 12065.